PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-208410

(43)Date of publication of application : 25.07.2003

(51)Int.Cl. G06F 15/00
G06K 17/00

(21)Application number : 2002-008180

(22)Date of filing : 17.01.2002

(71)Applicant : DAINIPPON PRINTING CO LTD

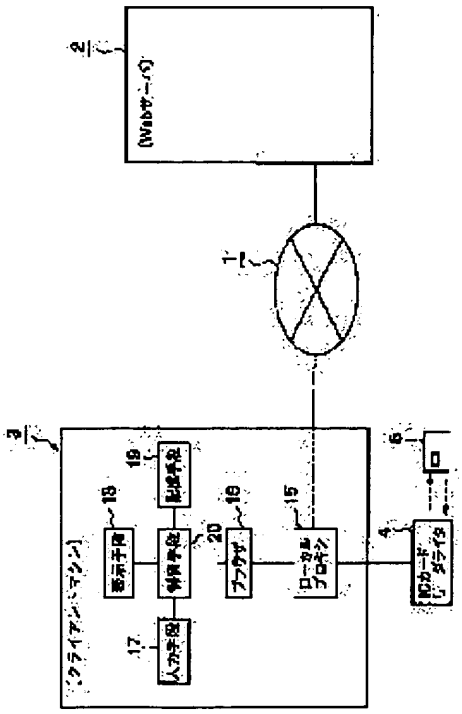
(72)Inventor : SAITO KENICHIRO

(54) AUTHENTICATION INFORMATION CREATING SYSTEM

(57)Abstract:

PROBLEM TO BE SOLVED: To provide an authentication information creating system capable of preventing the illegal access by a third person by allowing only a person having the access right to display a log-in form in which the log-in data is automatically inputted in advance.

SOLUTION: The authentication information creating system comprises an IC card storing the log-in data, an IC card reader/writer connected to a client machine, and the client machine having a local proxy for reading the log-in data stored in the IC card by the IC card reader/writer when the transmission of the log-in data is requested from a WEB server, and creating the display information of the log-in form in which the log-in data is inputted in advance by using the log-in data, and a browser receiving the display information of the log-in form from the local proxy for making a display means to display the display information of the log-in form.



LEGAL STATUS

[Date of request for examination] 14.01.2005

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報（Ａ）**　(11)特許出願公開番号
特開2003－208410
（P2003－208410A）
(43)公開日　平成15年７月25日(2003.7.25)

(51)Int.Cl.⁷	識別記号	ＦＩ		テーマコード（参考）
Ｇ０６Ｆ　15/00	３３０	Ｇ０６Ｆ　15/00	３３０Ｇ	５Ｂ０５８
Ｇ０６Ｋ　17/00		Ｇ０６Ｋ　17/00	Ｄ	５Ｂ０８５

審査請求　未請求　請求項の数２　ＯＬ　（全７頁）

(21)出願番号　特願2002－8180(P2002－8180)

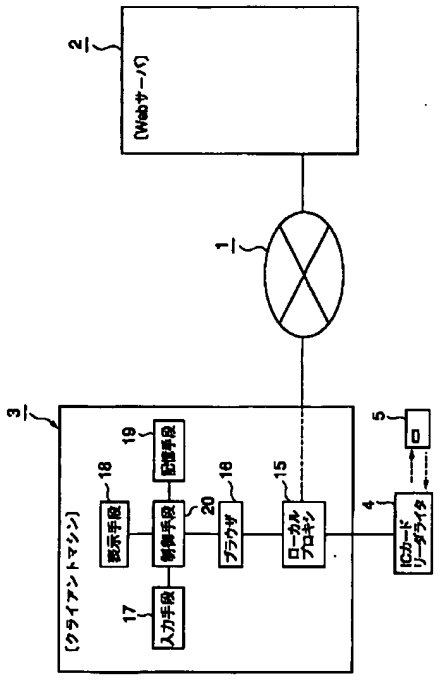
(22)出願日　平成14年１月17日(2002.1.17)

(71)出願人　000002897
大日本印刷株式会社
東京都新宿区市谷加賀町一丁目１番１号
(72)発明者　斎藤　賢一郎
東京都新宿区市谷加賀町一丁目１番１号
大日本印刷株式会社内
(74)代理人　100111659
弁理士　金山　聡

Ｆターム(参考)　5B058 CA01 KA02 KA04 YA20
5B085 AE02 AE03 AE12 BE01

(54)【発明の名称】　認証情報生成システム

(57)【要約】
【課題】　アクセス権を有する本人だけが自動的に予めログインデータが入力されたログインフォームの表示を可能とさせるようにすることで、第三者による不正なアクセスを防止できるようにした認証情報生成システムを提供する。
【解決手段】　ログインデータが格納されているＩＣカードと、クライアントマシンに接続されたＩＣカードリーダライタと、ＷＥＢサーバからログインデータの送信要求があった場合に、前記ＩＣカードリーダライタで前記ＩＣカードに格納されているログインデータを読み取らせ、該ログインデータを用いて予め前記ログインデータが入力されたログインフォームの表示情報を生成するローカルプロキシと、前記ローカルプロキシから前記ログインフォームの表示情報を受信し、表示手段に前記ログインフォームの表示情報を表示させるブラウザとを有する前記クライアントマシンと、からなることを特徴とする。



1

【特許請求の範囲】

【請求項1】　ＨＴＴＰアクセスを送信するクライアントマシンと、ネットワークを介して前記ＨＴＴＰアクセスを受信した後、アクセス権を確認するためのログインデータの要求信号を前記クライアントマシンに送信するＷＥＢサーバとにより、前記クライアントマシンが前記ＷＥＢサーバからログインデータの要求信号を受信した際における認証情報生成システムであって、

前記アクセス権を確認するためのログインデータが格納されているＩＣカードと、

前記クライアントマシンに接続され、前記ＩＣカードに格納されているログインデータを読み取るＩＣカードリーダライタと、

前記ＷＥＢサーバからログインデータの送信要求があった場合に、前記ＩＣカードリーダライタで前記ＩＣカードに格納されているログインデータを読み取らせ、該ログインデータを用いて予め前記ログインデータが入力されたログインフォームの表示情報を生成するローカルプロキシと、前記ローカルプロキシから前記ログインフォームの表示情報を受信し、表示手段に前記ログインフォームの表示情報を表示させるブラウザとを有する前記クライアントマシンと、

からなることを特徴とする認証情報生成システム。

【請求項2】　ＨＴＴＰアクセスを送信するクライアントマシンと、ネットワークを介して前記ＨＴＴＰアクセスを受信した後、アクセス権を確認するためのログインデータの要求信号を前記クライアントマシンに送信するＷＥＢサーバとにより、前記クライアントマシンが前記ＷＥＢサーバからログインデータの要求信号を受信した際における認証情報生成システムであって、

複数種類のＵＲＬと、前記各ＵＲＬ毎に対応したアクセス権を確認するためのログインデータが格納されているＩＣカードと、

前記クライアントマシンに接続され、前記ＩＣカードに格納されているＵＲＬとログインデータを読み取るＩＣカードリーダライタと、

前記ＷＥＢサーバからログインデータの送信要求があった場合に、前記ＩＣカードリーダライタで前記ＩＣカードに格納されている複数種類のＵＲＬの中から、その送信要求があったＵＲＬに対応して記憶されているログインデータを読み取らせ、該ログインデータを用いて予め前記ログインデータが入力されたログインフォームの表示情報を生成するローカルプロキシと、前記ローカルプロキシから前記ログインフォームの表示情報を受信し、表示手段に前記ログインフォームの表示情報を表示させるブラウザとを有する前記クライアントマシンと、

からなることを特徴とする認証情報生成システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、通信ネットワーク上の情報にアクセスし、このアクセス権を確認するためのログインデータの要求信号がＷＥＢサーバからクライアントマシンに送信された際に、前記クライアントマシンで前記ＷＥＢサーバに送信するためのログインデータを自動的に生成する認証情報生成システムに関する。

2

【０００２】従来、パソコン等のクライアントマシンを利用してインターネットに接続し、会員制などのサービスを受ける場合には、通常、Ｗｅｂブラウザを起動させ、キーボード等の入力手段から見たいホームページのＵＲＬを入力したり、またはブックマークに記録してあればそのＵＲＬを指定してＵＲＬを入力して、ＷＥＢサーバにアクセスを行なう。その後、ＷＥＢサーバからクライアントマシンに対して、ユーザＩＤやパスワード等の認証情報からなるログインデータの送信を要求する情報が送信され、これらのログインデータをクライアントマシンからＷＥＢサーバに送信し、照合判定を経た後に所定のサービスを受けることが可能となるようにしてある。

【０００３】一般的に、クライアントマシンのＷＥＢブラウザの機能として、前回のログイン時のログインデータを記憶しておき、次回以降におけるＷＥＢサーバからクライアントマシンに対するログインデータの送信要求があった際に、これらの記憶されているデータを自動的に用いることで、ＷＥＢサーバからログインデータの送信要求があった場合にその都度キーボード等の入力手段からユーザＩＤやパスワード等を入力しなくても処理できるようにして入力作業の手間を省くことを可能にしていることが多い。

【０００４】しかしながら、ＷＥＢブラウザの機能によっては、自動的にログインデータが入力される場合に、認証情報がソフトウェアで処理されるため、ログインデータが盗難される恐れがある。また、ユーザがブラウザを適切に設定していない場合、他人がブラウザを操作した時に、前回ユーザがログインした時のデータが自動的に入力されるため、第三者によるログインが容易となり、不正なアクセスが行われる危険性がある。

【０００５】更に、ブラウザ機能によるサポートがない場合、異なる複数のログインの要求に対してのアクセスを行なうには、それぞれの要求に対応したログインデータをキーボード等から入力しなければならず、手間がかかり、またこれらのログインデータをメモ書きなどの記録で管理しておくこともありセキュリティー上の問題がある。

【０００６】

【発明が解決しようとする課題】本発明は、クライアントマシンがＷＥＢサーバからログインデータの要求信号を受信した際に、アクセス権を有する本人だけが自動的に予めログインデータが入力されたログインフォームの表示を可能とさせるようにすることで、第三者による不正なアクセスを防止できるようにした認証情報生成シス

テムを提供する。更に、本発明は、異なる複数の要ログインの要求に対してのアクセスを行なう場合でも、それぞれの要求に対応したログインデータをキーボード等から入力しなくても、自動的にそれらに対応したログインデータが予め入力されたログインフォームの表示を可能とした認証情報生成システムを提供する。

【０００７】

【課題を解決するための手段】本発明の認証情報生成システムは、ＨＴＴＰアクセスを送信するクライアントマシンと、ネットワークを介して前記ＨＴＴＰアクセスを受信した後、アクセス権を確認するためのログインデータの要求信号を前記クライアントマシンに送信するＷＥＢサーバとにより、前記クライアントマシンが前記ＷＥＢサーバからログインデータの要求信号を受信した際における認証情報生成システムであって、前記アクセス権を確認するためのログインデータが格納されているＩＣカードと、前記クライアントマシンに接続され、前記ＩＣカードに格納されているログインデータを読み取るＩＣカードリーダライタと、前記ＷＥＢサーバからログインデータの送信要求があった場合に、前記ＩＣカードリーダライタで前記ＩＣカードに格納されているログインデータを読み取らせ、該ログインデータを用いて予め前記ログインデータが入力されたログインフォームの表示情報を生成するローカルプロキシと、前記ローカルプロキシから前記ログインフォームの表示情報を受信し、表示手段に前記ログインフォームの表示情報を表示させるブラウザとを有する前記クライアントマシンと、からなることを特徴とする。

【０００８】また、本発明の認証情報生成システムは、ＨＴＴＰアクセスを送信するクライアントマシンと、ネットワークを介して前記ＨＴＴＰアクセスを受信した後、アクセス権を確認するためのログインデータの要求信号を前記クライアントマシンに送信するＷＥＢサーバとにより、前記クライアントマシンが前記ＷＥＢサーバからログインデータの要求信号を受信した際における認証情報生成システムであって、複数種類のＵＲＬと、前記各ＵＲＬ毎に対応したアクセス権を確認するためのログインデータが格納されているＩＣカードと、前記クライアントマシンに接続され、前記ＩＣカードに格納されているＵＲＬとログインデータを読み取るＩＣカードリーダライタと、前記ＷＥＢサーバからログインデータの送信要求があった場合に、前記ＩＣカードリーダライタで前記ＩＣカードに格納されている複数種類のＵＲＬの中から、その送信要求があったＵＲＬに対応して記憶されているログインデータを読み取らせ、該ログインデータを用いて予め前記ログインデータが入力されたログインフォームの表示情報を生成するローカルプロキシと、前記ローカルプロキシから前記ログインフォームの表示情報を受信し、表示手段に前記ログインフォームの表示情報を表示させるブラウザとを有する前記クライアントマシンと、からなることを特徴とする。

【０００９】

【発明の実施の形態】以下、本発明の実施の形態を図面に基づいて詳細に説明する。図１は、本発明の一実施形態に係る認証情報生成システムの概略構成を示す図、図２は、本発明に使用するＩＣカードのブロック図、図３は、本発明に使用するＩＣカードの記憶内容を示す図、図４は、本発明の一実施形態に係る認証情報自動生成システムの概略的なブロック図、図５は、本発明の一実施形態に係る認証情報生成システムのクライアントマシンにおけるログイン画面の一例を示す図、図６は、本発明の一実施形態に係る認証情報生成システムの処理手順を示すフローチャートである。

【００１０】図１に示すように、インターネット１上には、種々のサービスや情報を提供する複数のＷｅｂサーバ２ａ，２ｂが接続されると共に、これらのＷｅｂサーバ２ａ，２ｂからサービスや情報の提供を受けるためのパソコン等からなるクライアントマシン３が接続されている。このクライアントマシン３には、ＩＣカードリーダライタ４が接続され、ＩＣカードリーダライタ４にセットされたＩＣカード５に記憶されたデータの読み取りを可能にしてある。

【００１１】ＩＣカード５には、図２に示すように、制御手段であるＣＰＵ６、記憶手段として備えられた読み出し専用メモリ（ＲＯＭ）７ａと、書き換え可能な不揮発性メモリ（ＥＥＰＲＯＭ）７ｂと，揮発性メモリ（ＲＡＭ）７ｃとを有する。また、更にＩＣカード５には、電源電圧を供給するＶＣＣ端子８、接地用のＧＮＤ端子９、リセット信号を供給するＲＳＴ端子１０、クロック信号を供給するＣＬＫ端子１１、データ入出力手段であるＩ／Ｏ端子１２とがそれぞれ備えられている。そして、上記のＣＰＵと各メモリと各端子は、ＩＣモジュール化されてカード基材に埋設された構成を有している。

【００１２】また、不揮発性メモリ（ＥＥＰＲＯＭ）７ｂには、図３に示すような内容の情報が記憶されている。この記憶情報としては、インターネットを介して接続されるＷｅｂサーバのホームページのアドレスであるＵＲＬ１３ａと、このアドレスに接続する際に必要な認証情報として予めＷｅｂサーバ側に登録してあるユーザＩＤ１３ｂ及びパスワード１３ｃとが関連情報として記憶されている。

【００１３】更に、クライアントマシンの利用者が複数のＷｅｂサーバからサービスや情報の提供を受ける場合には、必要に応じてその他のＷｅｂサーバのホームページのアドレスであるＵＲＬ１４ａと、このアドレスに接続する際に必要な認証情報として予めＷｅｂサーバ側に登録してあるユーザＩＤ１４ｂ及びパスワード１４ｃなどを記憶させる。これにより利用者は、１枚のＩＣカード５をＩＣカードリーダライタ４にセットするだけで、複数のＷｅｂサーバに対応したログインデータの自動入

力処理を行なうことができる。

【００１４】次に、図５のブロック図に基づいて、本発明のシステム構成を説明する。クライアントマシン３には、ユーザ接続のインターネット・ゲートウェイ端部において、ローカルプロキシ（ｐｒｏｘｙ）１５というアプリケーションと、Ｗｅｂブラウザプログラム１６とが備えられている。また、更にキーボード等からなる入力手段１７と、ＣＲＴ等の表示手段１８と、記憶手段１９と、制御手段２０とを備えている。

【００１５】クライアントマシン３とＷｅｂサーバ２との間の通信は、ローカルプロキシ１５を経て行われ、ローカルプロキシ１５からの要求に基づいてＩＣカードリーダライタ４がＩＣカード５に記憶された所望の情報を読み取り、この情報をローカルプロキシ１５へ送信するようにしてある。つまり、利用者がＷｅｂサーバ２からサービスや情報の提供を受ける際において、クライアントマシン３の入力手段１７からＵＲＬの入力または画面上からＵＲＬを特定する指示情報を入力し、ブラウザを起動することでこのＵＲＬとブラウザの情報とをローカルプロキシ１５を経て、インターネット１を介してＷｅｂサーバ２に送信する。

【００１６】また、これらの情報を受信したＷｅｂサーバ２では、要求されたＵＲＬに該当するホームページをクライアントマシン３に送信する前提として、利用者の認証情報の照合が必要な場合には、Ｗｅｂサーバ２からクライアントマシン３に対して、利用者のユーザＩＤやパスワード等の認証情報からなるログインデータの送信を要求するためのログイン要求情報が送信される。

【００１７】ローカルプロキシ１５では、Ｗｅｂサーバ２から受信したデータとして、ログインデータを入力する必要の有無をチェックし、もしログインデータを入力する必要があるとするログイン要求情報が含まれている場合には、ＩＣカードリーダライタ４に対して、ＩＣカード５に記憶されたユーザＩＤ１４ｂ及びパスワード１４ｃなどの認証情報を読み取らせて、ローカルプロキシ１５に送信させる機能を有する。また、Ｗｅｂサーバ２から受信したデータにログイン要求情報が含まれていない場合には、そのデータはそのままをブラウザ１６に送られる。

【００１８】そして、ローカルプロキシ１５は、サーバから受信したデータを編集したログインフォームに、ＩＣカード５から読み出した認証情報を使用して、既にユーザＩＤやパスワード等の認証情報が設定された状態のログインフォームを作成し、ブラウザ１６に送信する機能を有している。ブラウザ１６は、ローカルプロキシ１５から受信した既に認証情報が設定された状態のログインフォームを表示手段１８により、図５に示すようなログイン画面２１として表示させる。

【００１９】図５に示すログイン画面２１では、ユーザＩＤ表示部２２やパスワード表示部２３等の認証情報の表示部と、これらの情報をログインデータとして、クライアントマシン３からＷｅｂサーバ２に送信することを認めるためのログイン送信ボタン２４が表示される。尚、ログイン画面２１のパスワード表示部２３には、セキュリティー上の安全性を考慮して具体的な文字や番号の表示が行われないようにしておく。

【００２０】また、クライアントマシン３が複数種類の異なるＵＲＬとアクセスする場合においては、各ＵＲＬ毎に対応したアクセス権を確認するための認証情報であるログインデータをＩＣカード５に格納しておく。つまり、図３において、記憶情報としてインターネットを介して接続されるＷｅｂサーバのホームページのアドレスであるＵＲＬ１３ａと、このアドレスに接続する際に必要な認証情報として予めＷｅｂサーバ側に登録してあるユーザＩＤ１３ｂ及びパスワード１３ｃとが関連情報として記憶され、また別のＷｅｂサーバのホームページのアドレスであるＵＲＬ１４ａと、このアドレスに接続する際に必要な認証情報であるユーザＩＤ１４ｂ及びパスワード１４ｃとが関連情報として記憶させておく。

【００２１】この場合、ローカルプロキシ１５では、Ｗｅｂサーバ２から受信したデータ又はＷｅｂサーバ２から送信した際のデータの中から、ＷｅｂサーバのホームページのアドレスであるＵＲＬを特定しておき、もしＷｅｂサーバ２から受信したデータにログイン要求情報が含まれている場合には、ＩＣカードリーダライタ４に対して、ＩＣカード５に記憶されたＵＲＬに対応して記憶されたユーザＩＤ及びパスワードなどの認証情報を読み取らせて、ローカルプロキシ１５に送信させる機能を有する。これにより、１枚のＩＣカードにより複数の異なるＵＲＬに対応することが可能となる。

【００２２】次に、図６のフローチャーを参照して、本発明の一実施形態における認証情報生成システムの処理手順を説明する。まず、利用者は、自分のＩＣカード５をＩＣカードリーダライタ４にセットする（Ｓ１）。そして、クライアントマシン３の入力手段１７から、アクセスを行ないたいホームページのＵＲＬの入力又はブックマークに記録してあるＵＲＬの指定入力を行ない、このＵＲＬをＷｅｂサーバ２に送信する（Ｓ２）。これの対し、Ｗｅｂサーバ２からクライアントマシン３に対して、利用者のユーザＩＤやパスワード等の認証情報からなるログインデータの送信を要求するためのログイン要求情報が送信される（Ｓ３）。

【００２３】そのログイン要求情報を受信したクライアントマシン３のローカルプロキシ１５は、ＩＣカードリーダライタ４に対して、ＩＣカード５に記憶されたこのＵＲＬに関連させて記憶されたユーザＩＤ及びパスワードなどの認証情報を読み取らせて、送信させる（Ｓ４）。この認証情報を受信したクライアントマシン３のローカルプロキシ１５は、サーバから受信したデータを編集したログインフォームに、ＩＣカード５から読み出

した認証情報を使用して、既にユーザＩＤやパスワード等の認証情報が設定された状態のログインフォームを作成し、ブラウザ１６に送信する（Ｓ５）。

【００２４】ブラウザ１６では、表示手段１８に認証情報が設定された状態のログインフォームが表示されたログイン画面を映す（Ｓ６）。利用者は、このログイン画面のログインフォームを確認し、ＯＫであれば「ログイン」の表示部分をクリックする（Ｓ７）。クライアントマシン３からＷｅｂサーバ２に対して、これらのユーザＩＤやパスワード等の認証情報からなるログインデータが送信される（Ｓ８）。以上の手順により、ログイン処理の際に利用者のＩＣカード５に記憶されたユーザＩＤ及びパスワードなどの認証情報を読み取らせて、ログインデータとして用いることができるものである。

【００２５】

【発明の効果】以上説明したように、本発明の認証情報生成システムは、クライアントマシンがＷＥＢサーバからログインデータの要求信号を受信した際に、利用者が所持するＩＣカードに記憶された認証情報を利用して、自動的に予めログインデータが入力されたログインフォームが表示されたログイン画面を表示手段に映し出すことができ、このログイン画面からログインデータの送信指示を行なうことができるので、第三者による不正なアクセスを防止することができるという効果がある。更に、本発明は、ＩＣカードに異なる複数のＵＲＬに対応させた認証情報を記憶させているので、複数の異なる要ログインの要求に対しても、それぞれの要求に対応したログインデータをキーボード等から入力しなくても、自動的にログインデータが予め入力されたログインフォームをログイン画面に表示することができるので、第三者による不正なアクセスを防止すると共に、作業効率がよいという効果がある。

【図面の簡単な説明】

【図１】本発明の一実施形態に係る認証情報生成システムの概略構成を示す図である。

【図２】本発明に使用するＩＣカードのブロック図である。

【図３】本発明に使用するＩＣカードの記憶内容を示す図である。

【図４】本発明の一実施形態に係る認証情報生成システムの概略的なブロック図である。

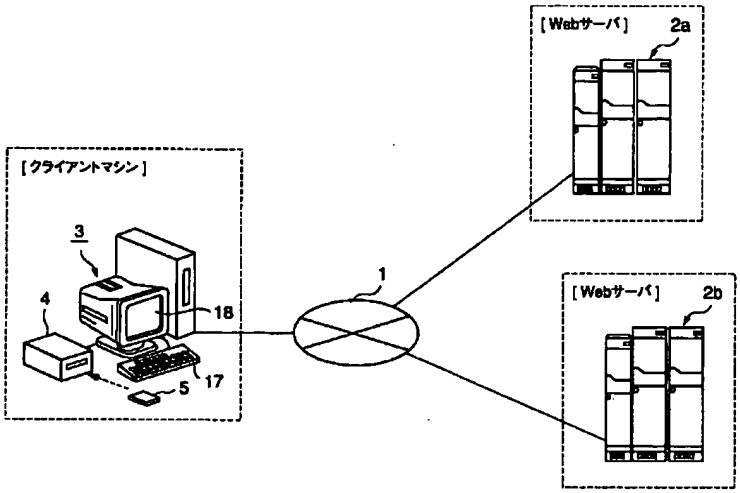
【図５】本発明の一実施形態に係る認証情報生成システムのクライアントマシンにおけるログイン画面の一例を示す図である。

【図６】本発明の一実施形態に係る認証情報生成システムの処理手順を示すフローチャートである。

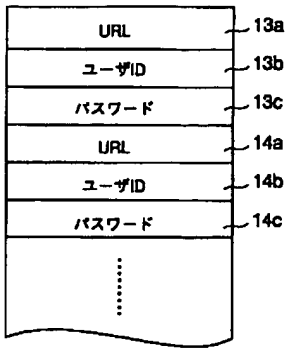
【符号の説明】

１　インターネット
２ａ，２ｂ　Ｗｅｂサーバ
３　クライアントマシン
４　ＩＣカードリーダライタ
５　ＩＣカード
６　ＣＰＵ
７ａ　読み出し専用メモリ（ＲＯＭ）
７ｂ　不揮発性メモリ（ＥＥＰＲＯＭ）
７ｃ　揮発性メモリ（ＲＡＭ）
８　ＶＣＣ端子
９　ＧＮＤ端子
１０　ＲＳＴ端子
１１　ＣＬＫ端子
１２　Ｉ／Ｏ端子
１３ａ　ＵＲＬ
１３ｂ　ユーザＩＤ
１３ｃ　パスワード
１４ａ　ＵＲＬ
１４ｂ　ユーザＩＤ
１４ｃ　パスワード
１５　ローカルプロキシ
１６　ブラウザ
１７　入力手段
１８　表示手段
１９　記憶手段
２０　制御手段
２１　ログイン画面
２２　ユーザＩＤ表示部
２３　パスワード表示部
２４　ログイン送信ボタン

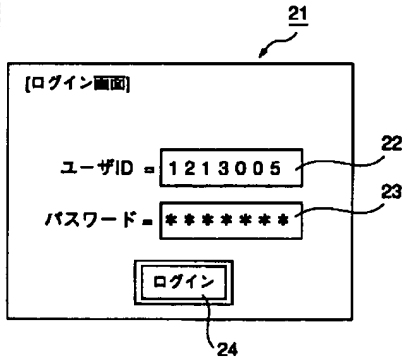
【図１】


[Webサーバ]
2a
[クライアントマシン]
3
4
18
1
5
17
[Webサーバ]
2b

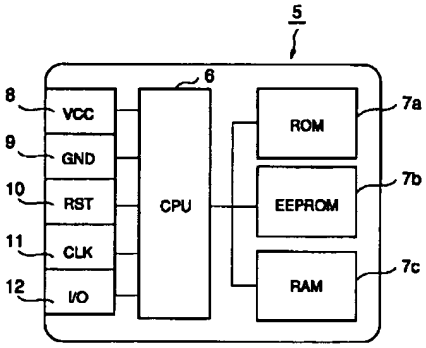
【図３】


URL
13a
ユーザID
13b
パスワード
13c
URL
14a
ユーザID
14b
パスワード
14c

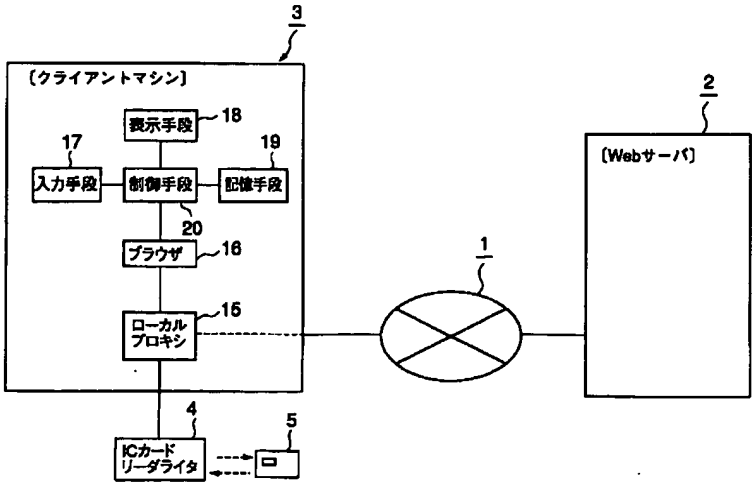
【図５】


21
[ログイン画面]
ユーザID =
1213005
22
パスワード =
****
23
ログイン
24

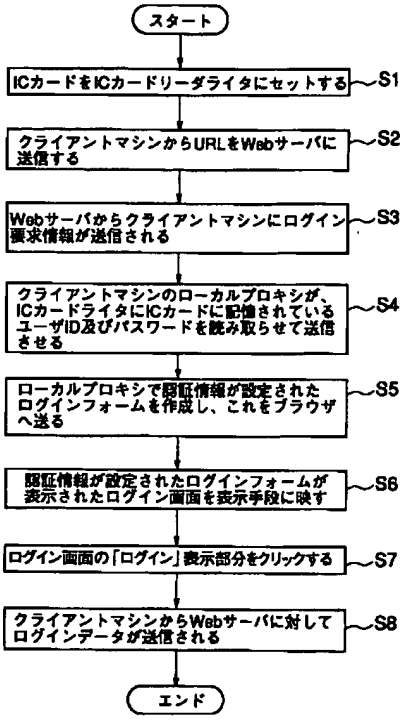
【図２】


5
6
8
VCC
9
GND
10
RST
11
CLK
12
I/O
CPU
ROM
7a
EEPROM
7b
RAM
7c

【図４】


3
[クライアントマシン]
表示手段
18
17
入力手段
制御手段
19
記憶手段
20
ブラウザ
16
ローカル
プロキシ
15
4
ICカード
リーダライタ
5
1
2
[Webサーバ]

【図6】


スタート
ICカードをICカードリーダライタにセットする
S1
クライアントマシンからURLをWebサーバに送信する
S2
Webサーバからクライアントマシンにログイン要求情報が送信される
S3
クライアントマシンのローカルプロキシが、ICカードライタにICカードに記憶されているユーザID及びパスワードを読み取らせて送信させる
S4
ローカルプロキシで認証情報が設定されたログインフォームを作成し、これをブラウザへ送る
S5
認証情報が設定されたログインフォームが表示されたログイン画面を表示手段に映す
S6
ログイン画面の「ログイン」表示部分をクリックする
S7
クライアントマシンからWebサーバに対してログインデータが送信される
S8
エンド